Center for Strategic and International Studies

Cyber Disrupt 2017

"Keynote: Next Steps for Cybersecurity After a Decade of Lessons Learned"

Introductions:
Frances F. Townsend,
Executive Vice President,
MacAndrews & Forbes Incorporated

Denise E. Zheng,
Director and Senior Fellow, Technology Policy Program,
CSIS

Keynote:
Thomas Bossert,
Assistant to the President,
Homeland Security and Counterterrorism

Location: CSIS Headquarters, Washington, D.C.

Time: 9:00 a.m. EDT
Date: Wednesday, March 15, 2017

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

DENISE E. ZHENG: And welcome to CSIS for our first-ever Cyber Disrupt Summit. My name is Denise Zheng. I'm the director of the Technology Policy Program here at CSIS and a senior fellow. We are – we are very pleased to be hosting you today for a day of very dynamic, substantive, timely conversation about strategies, policies, and technology practices that will be disruptive to the current status quo and improve cybersecurity. We'll have a day of keynotes, panels, TED Talks, and a live active interactive debate at the very end just to cap things off.

I also do want to take a moment to thank our sponsors. This event would not have been possible without support from the Smith Richardson Foundation, Tanium, Symantec, ForeScout, Intel Security, and Raytheon.

It is also my honor to introduce Fran Townsend. She needs no introductions, of course, but Fran is former homeland security adviser to President George W. Bush. She also served as deputy national security adviser for combatting terrorism from 2003 to 2004. She's spent 13 years in the U.S. Department of Justice and the administrations of Presidents H.W. Bush, Bill Clinton, and George W. Bush. Ms. Townsend is currently executive vice president for worldwide government, legal and business affairs at MacAndrews and Forbes Incorporated. And of course, we all know Fran from her frequent appearances on CBS News and CNN. She's also a member of the CSIS family, having joined our board of trustees in 2005.

So please join me in welcoming Frances Townsend. (Applause.)

FRANCES F. TOWNSEND: Good morning, everybody. Thank you for coming out. The weather cooperated with us, so I am pleased we're all – you're all here. I apologize. We're off to a little bit of a late start.

You know, I remember back to when I sat in Tom's seat and we were grappling with the cybersecurity challenges, and they've only magnified. And frankly, the threat is far worse today and goes to the fundamental security of our federal infrastructure and our information security.

It's clear that the Trump administration knows that cybersecurity is a central challenge both for domestic and foreign policy. It is a key issue for our economic health and our national security, and so I couldn't be more pleased to introduce Tom Bossert, who is now the assistant to the president for homeland security and counterterrorism. I work – I had the privilege of working with Tom when I was at the White House, and he comes to the – to the job now with exactly the right experience. He was my deputy. He was the deputy assistant to the president for homeland security, where he advised President Bush on homeland security, counterterrorism, and the continuity of operations. He worked on the Comprehensive National Cybersecurity Initiative, our nation's first effort to build better cybersecurity, elements of which we still use today. Tom can tell us about how the threat landscape has changed since the CNCI, what the challenges in cyberspace does for the – that the United States confronts today, and how the administration's cybersecurity strategy will address those threats.

Please join me in welcoming Tom Bossert. (Applause.)

THOMAS BOSSERT: Thank you all very much, and I apologize for being tardy here today. It's entirely my fault and not Fran's, which is a flip reverse of our normal responsibility with one another. (Laughter.)

A few lighthearted comments first, if I could. I've now inherited Fran's old office. And for Fran and Lisa Monaco, my predecessor, that was a comfortable environ. For me it is the shortest office in the White House, and I'm the tallest staffer occupying it. (Laughter.) So, for those of you that haven't been to the office, please, over the next however many years I'm privileged to serve President Trump, make it an effort to stop by and visit me, and I will be glad to host you there, provided there's no Essex bar on that visit. If there is, don't come. Go talk to Fran. (Laughter.) And we'll take care of our cybersecurity together as a nation.

So let me introduce a few thoughts, but let me start by thanking the hosts here and thanking a few others. So Fran was fairly modest there. Fran has been responsible for my series of promotions in my career. So I would observe first that I've been a policy director, a senior director, a special assistant to the president, a deputy assistant to the president, all under Fran Townsend. And now I've had the privilege to be an assistant to the president and Homeland Security adviser under President Trump.

So I am quite privileged to be here, but I'm quite privileged to be in this job. I think that's the most important thing for me to convey to the public today. I take this responsibility seriously. I'm here for the mission. I'm not here for me. I've now achieved everything I ever want to achieve in life. I am done, when this job is done, with public service. And I take it very seriously. I don't get too caught up in all of the public mesaginations (sic) about who's doing what with whom. Right now I work for the president. He's given me clear guidance. There is no problem with that guidance. And I want to start by telling you what that guidance is. I see some friends in the room.

The guidance to me started in terms of priorities before I took the job. And for those of you that haven't seen the now-leaked draft executive order, I'll address that directly. But it starts with a commentary on us operating our federal networks on behalf of the American people. That is President Trump's view. That is his personal view. That is a view that he communicated to me in the interview process for this job. That is not a platitude. And he doesn't view it kindly that we have bureaucrats viewing this as a responsibility among others and questions about priorities. It is an absolutely solemn responsibility. And from his perspective, if we can't do it better, he'll be very frustrated.

So, to me, I want to introduce some priorities. And those priorities start with those things that we can control the most and the most directly. And the most directly controllable thing for President Trump and I to control are federal networks and their data. So federal networks and data is the first priority for us. I'll walk through some details there on how we plan to address that. And priority two, only by function of it having to be number two, our critical infrastructure. But not all critical infrastructure is equally critical, so we will focus in on the most critical of those things, what some of us refer to as Section 9 entities.

And then, three, we need to tackle the notion of securing our nation and the American people. And cybersecurity is the area where we talk about it quite a bit, but we have not yet gotten serious about a serious deterrent strategy. And so the idea, from my perspective, is to take the Cabinet, bring them together very seriously, as we negotiate with our foreign enemies and frenemies and enemies, and figure out how we're going to share information responsibly with our allies and how we are going to deter our adversaries. That is a stated objective. This administration will take it seriously. And we will be looking for achievable ideas to that end. I think that needs to be stated out loud.

So that's the theory of my case. Let me go back and prove a little bit of what we intend to do. I'm excited about it. I think we can achieve it. But we cannot achieve it without partnership –

partnership with you, partnership with industry, partnership with the owners and operators of infrastructure, and, frankly, partnership within our governments, state and local governments, and even internal to our federal enterprise, which is designed, as many of you know, with interagency as a noun. So my job here is to make sure that that becomes a coordination function and not a noun.

I've given my speech away. Let me come back and thank Jim Lewis and Denise Zheng, in addition to Fran Townsend. Denise and Jim have been leaders in this field. I'd like to thank Chairman McCaul and Senator Whitehouse. They've been leaders in this field. They've led this effort. They've led recommendations. They've led what has brought us here today to this summit, a policy task force. We've reviewed that in the White House. We've reviewed their recommendations and taken them quite seriously.

There have been 15 reports with 175 collective recommendations from CSIS to Misters Donilon and Palmisano and the Commission, Cybersecurity Commission. I've spoken to most of the leaders of those operations, summits, reports, commissions, authors of those reports; 175 recommendations. All boil down to the same four things that I started out with as our recommendations. And I can promise you that I came up with those four priorities before I read 175 recommendations. And so I view it as a validation, to some degree, of what we've all been doing together as a group.

And I've jokingly said this at breakfast, but Jim Lewis wrote a report in 2009 that I make the 16th. It's not recently released, but it's still equally prescient and it's still, in large part, something that we should look at implementing today. That is not a criticism of where we've come or what we've not done over the last eight years, but it's an observation, to Fran's point, that as I come back to this world, I feel like I have re-awoken from a long eight-year nap and I have found a world that is on fire, to some degree. The cyberthreat has magnified. The terrorism threat has magnified. They are the same threats. They are the same phenomenon. But they are on a scale that is much wider, much larger, with a greater cost.

So, with that sombering note, federal networks. Federal networks at this point can no longer sustain themselves. We cannot tolerate indefensible technology, antiquated technology, hardware and software. Modernization is absolutely critical. We will pursue that. You will see details in the coming weeks and months on how we will pursue that. It is not easy, but we cannot any longer defend indefensible networks.

Second priorities. We've had some confusion, and I want to clarify it, on who's responsible for what. Federal agency heads will be held responsible and accountable to the president, as they should have been, I think, I believe have been for the last 10, 12 years, for their own enterprise network security.

However, also, not an or, not an instead of, but in addition to, we will hold the entire federal network as an enterprise and view it as something that needs to be defended as such. We can no longer dream away the notion that we will have cybersecurity expertise in terms of capital investment and human investment resident at 190 or 220 federal agencies. It would be very difficult to achieve and sustain that, and it would be unwise for us to attempt to do it on behalf of the taxpayer. So shared services will be a fundamental requirement. How we achieve that will require some time, and we'll come out with some details as we move forward.

Secondly, in addition to modernization and shared services, we have to look at this enterprise risk in a national-security holistic manner. We often talk about OPM. There's going to be a strong

push to manage our risk using the framework. Most of you will have heard that before. Frankly, I think it's a good idea.

But the second question is going to become what are our metrics? We're aware that we need metrics. And I'll use that word here so that you don't accuse me of not knowing what I'm talking about. Those metrics, though, will be something that we know when we see them. OPM is a good example, because we all know that now, in retrospect, as having been an obvious metric. We had crown jewels in a system, held responsibly in some ways by an OPM director who had been in charge of her own or his own, depending on who our next OPM director will be, enterprise.

However, on behalf of the federal enterprise, on behalf of our national security, additional effort, additional money and additional defenses should have been applied to those crown jewels. We will require agency heads to communicate that information to the White House so that DHS can apply their operational observations, skill sets and applied sciences, and that OMB can apply its financial and administrative skills, and we can make a determination on how to more adequately deflect our adversaries and affect our cybersecurity investments.

Side point here. This week I mentioned health care as President Trump's priority, as it should be. I think what you'll also see is on Thursday a budget blueprint. So as to not get caught up in the executive-order questions that you have, I'll direct you to this Thursday's rollout. President Trump intends to put his money where his mouth is. There will be a budget request to the Hill that will reflect his view that we need greater defense readiness, but also greater security. Cybersecurity will be part – is part. You will see on Thursday when he releases it. It is part of his budget request.

Cybersecurity will be funded through DOD and DHS. Homeland Security will be funded. Defense will be funded. This is not just simply an exercise in defense readiness. This is an exercise in protecting America. I don't want to get too far out in front with numbers, but that's a tease for you for Thursday, certainly.

I've got one more thank-you to offer, and that is to the staff who have put this together. The staff who put this summit together have reached out to me in small and large ways and made me understand each and every one of you, what your concerns are. And so I want to take you to some of the more detailed nuances of what might be an executive order.

One of them is botnets, and this is something I'm a little bit concerned about. I believe – and if the staff work is correct, this might resonate with this room – I believe that we can radically reduce the number of botnets of this country. I believe that that's a voluntary effort, and I'd like us to call for that publicly. The president will call for that publicly. We need an effort that no longer looks at the bottom of the mountain but that rather looks in a higher topography order to get to the root cause of some of these botnet attacks.

It's going to require the collaborative cooperation of companies – as you know, not only ISP providers by companies by name. Some are social media companies. Some are Internet search engines. But collectively, that information can be readily assessed, readily digested.

And botnet attacks can be reduced; if not to zero, we can dramatically reduce their number if we put our minds to it. So this will a call to voluntary coordination and a call to our leadership goal. And we'll provide the mechanism to coordinate that effort.

And then, lastly, I would invite you, Democrats, Republicans – there is no partisanship in this issue. This issue is about deterring our enemies. So, as we move to section three of what will most likely be an executive order in the coming weeks or months, we need to look at sharing with our allies, but we need to also look at deterring their intent.

So that's how I started, deterring our adversaries. That's how I'll end, deterring our adversaries. I'm not sure how I'm doing on time. I could talk for about 20 more minutes. But Fran, if you'd like to, we can talk details.

MS. TOWNSEND: Sure. Why don't we have a conversation.

MR. BOSSERT: Thank you very much. (Applause.)

MS. TOWNSEND: Tom, thank you for that. Let's – let me take you back. You mentioned the three priorities. When you talk about the federal network and modernization and shared services, give us a sense of – you've got a budget coming. Modernization's got a big price tag across the federal government. And it's not a – it's not a single budget year project. How do you think about that and getting your arms around the modernization of the federal infrastructure?

MR. BOSSERT: Yeah, that's a good question.

So I think there's three answers there. There will not be a budget that reflects an overnight modernization of the IT. I think that's somewhere around a $90 billion endeavor that's going to require more time, a little bit more thoughtful analysis. We're I think 60 days into this administration, so we'll get there. I think we've demonstrated quite a bit of success in 60 days, despite all the fanfare.

That said, the money in the defense investments and the homeland security investments that I spoke of are meant to direct towards current efforts but also renewed efforts that have never been quite implemented the right way. So that money will have to be followed by policy guidance, thoughtful leadership at the Department of Homeland Security. Secretary Kelly and others have demonstrated to me a great deal of confidence and competence in this matter.

But there are some tactical parts of your question there as well. We've seen spear phishing. I think CrowdStrike and Verizon and FireEye and others have all come out with their reports. And they still seem to say the threat vector of today is spear phishing. It looks as – I looked at them – as if it's becoming more complex. There are phone calls preceding well-crafted emails, and the tradecraft is improving. The success rate is good. So those are low-hanging tactical issues.

Major reforms of a budgetary nature, we're going to – going to require years of investment. And so the third point there, and that's the interim midterm point: As we assess risk, which is not just a function of requiring departments and agencies to report to us their risk management activities, it's also a function of them reporting to us that risk, which they're aware of, and that they are – they are not mitigating. That is something we have not done before: Reporting your known and unmitigated risk will be a requirement moving forward.

We are already beginning that effort. That's going to require an obvious reaction. And the obvious reaction is, if you want us to mitigate it, and we don't have any more money to do so, how would you like us to handle it? That requires greater importance and greater investment, rather, than DHS' capabilities as a quasi-shared service provider and their function and role. But it also requires us

to have the ability to meet those unmet needs. And that's a budget mechanism as much as it is an additional budget cost item.

We can't predict what that will be. For those of you that are defense-oriented, we have an OCO budget. For those of you that are homeland security-oriented, we have a DRF. For those of you that are cybersecurity-oriented, we've had attempts in the past to develop a revolving fund. None of them have quite stuck in this application. But we do need to address unmet needs in a budgetary matter in a regular ongoing basis as we assess risk and determine insufficiencies on behalf of the entire federal network as opposed to some individual agency process where we hold them accountable but then don't necessarily give them the money and resources to carry out all of their missions in addition to their cybersecurity responsibilities. So that's not a call for more money. It's a call for efficiency. It's tied hand in hand with modernization. Modernization is going to have a big price tag. But in the interim, we're going to need a way to meet unmet needs with unrealized threats and unmitigated risks, if that makes sense.

So that's kind of a three-part answer.

MS. TOWNSEND: So the tricky part to this, right, is because of the way the budget process works, both internal to the executive branch and on the Hill, you're going to need the support of some your congressional allies. You rightly called out and thanked Chairman McCaul and Senator Whitehouse. Do you – do you think you can get the support on Capitol Hill that you're going to need for the kind of budget flexibility that requires?

MR. BOSSERT: The answer to that is yes. I'm a little out over my skis to say that. I don't want to begin to list the number of senators and congressmen and congresswomen that I've called because I'll omit one. I've called out two here today for the specific purpose of thanking them for their leadership on the effort and the task force that they've led here at CSIS. But I have talked to, in my mind – and if I haven't talked to you yet, and you're watching this, I will call you shortly – every important and unimportant and there is no such thing member of Congress, Senate, House, their staffs, appropriations committees, authorizing committees.

And every single person I talk to, those that understand cybersecurity and those that just read about it in the paper, agree that we need some reform. And that's the start. If they disagreed and they thought it wasn't a problem, I would say no to you or I would say maybe. But every single person of both political stripes, some independents, some former independents that aren't in Congress or in the Senate anymore, have all agreed, and they've all given me advice, and they've all said that we have to do something. I've demonstrated hopefully some competence on the matter, some care and some zeal and passion on the matter. And they've committed to me at least verbally to helping us.

Now, that puts the responsibility and the awesome task back on me. President Trump has now said this is a priority, and we need to take care of it; yes, sir. In the Congress and those that have supported have now said, come out with a thoughtful approach that we can get behind and implement; yes, ma'am, yes, sir.

So now we have two calls to action. I need a staff and a – and a support structure within the entire federal government. Secretaries Mattis and Secretary Tillerson and Secretary Kelly and others are going to be instrumental in this effort. But I also need the people in this room. It's not a platitude to come out with good ideas and to shorten those 175 recommendations into things that we can achieve. And I believe that the executive order President Trump will issue will provide a mechanism within

which you can plug all your recommendations. There is three sections, and there is three categories of your 175 recommendations. And that's not – that's not an accident.

MS. TOWNSEND: So tell me, you mentioned that there will be metrics associated with this. Are those – and that the Cabinet agency heads will be held accountable. Are they metrics that will be made public, or is it internal metrics by which you'll measure progress?

MR. BOSSERT: Yeah, I – thank you. Couple of thoughts here. I think that I'm often guilty of having sat at your seats, and I listen to speakers, and I write down critical thoughts. What didn't he or she say? Metrics is something I've always written down. So I addressed it, but I shouldn't have focused on it.

The answer here is that we're going to go through a thoughtful approach that requires federal departments and agencies to adopt and implement the cybersecurity framework developed by NIST and any subsequent iteration of that document. They're going to be required to produce for us a report – and when I say us, ultimately, the president, but it's going to go through the security of homeland security first and foremost, under FISMA contemplated law and actual law, but under the contemplated construct of FISMA, the secretary of homeland security is going to provide the expertise to look at that and to digest the technical construct of that. It's going to go through OMB so that they can look at it from a management perspective. And it's going to go to the president through me, in most cases.

And the idea there is for us to collectively render determinations on the adequacy those mitigations strategies as management tactics. But also then it's going to have to be done in some way as a – as a scorecard, right? How do we decide whether we've determined adequacy or sufficiency? We're going to have to develop metrics. So we don't have them.

And whether they're public or not, I think probably not because the idea here of defending the collective federal enterprise as opposed to the agency and department enterprises, the idea is to defend our crown jewels from a national security perspective. And that will inherently will be something that we don't want to reveal to the public or our enemies.

But that effort of developing those metrics has to be acknowledged as we work through that process. I mentioned OPM because it's an easier metric to wrap your mind around. I'll know it when I see it, that standard, but we all now know that a(n) antiquated hardware system and an antiquated database software system holding millions and millions of important records to our national security was a bad approach. That was known and unmitigated risk, contemplated through the lens of one agency who had responsibility for their enterprise. It now needs to be looked at through the lens of the security of our nation and it has to be examined in addition to each agency – in addition – it has to be examined at a White House level to make sure that we've got a collective.

MS. TOWNSEND: Now, to undertake an endeavor of this magnitude, you need the right talent.

MR. BOSSERT: Yeah.

MS. TOWNSEND: You need it at the White House. You need it at DHS and the departments and agencies. How do you – how do you go about recruiting, retaining? It is – it – this was a challenge in the Bush administration, in the Obama administration, for every administration. Talk to me – talk a little bit about recruiting and keeping talent.

MR. BOSSERT: Yeah, I think there's – it's difficult for the federal government in any field to recruit and retain talent. There's a lot of money, there's a lot of opportunities, there's a lot of fun in the private industry, and so people end up through a revolving door. So I think we need to concede a managed service – a managed service provider model – sorry – is the model that we're going to have move towards. And so when I talk about managed services, I talk about managed services in terms of cloud services, but also in terms of security services. And I think that we're going to have to acknowledge that DHS is playing a little bit of a managed service role to its compatriot departments and agencies and that they're going to have to reach out and get those resources from private industry and be receptive to that revolving door to some degree.

Now, that carries with it some thoughtful engineering. That thoughtful engineering is going to have to involve some procurement modification. That procurement modification is going to have to require a budget. So this is all an interrelated layered risk management exercise.

But I would say maybe one or two more things on that. I thank Chairman McCaul, but I think that DHS needs to do a hard internal assessment of its capacity and capabilities to meet its mission. That's not a negative. That's not a criticism. It's just a thought and a recommendation for DHS as they move forward. Their leadership's already engaging in that effort. And I think some of the money and some of the resources that the president provides to the Department of Homeland Security to do that, will have to be spent on human capital, not just on capital investments and things.

And then lastly, I would reiterate my – I would reiterate my observation that we can't have resident in 190 or more federal agencies the same level of zeal, passion, capacity and capability that we can have in centralized places that provide managed services. It's the job of some of us to provide cybersecurity. I'm the policy coordinator, I'm the integrator, and we don't have any operational capacity at the White House and I don't intend to ever, while I'm there, seek it. I don't think we would have the right money, the right skillset, and I think it would probably be a mistake for a lot of reasons. So with DHS and with OMB helping us assess risk, we will then task back out to the departments and agencies, and we will rely heavily on private industry. I think that's the only way to get and retain talent.

MS. TOWNSEND: You know, their – today we know that the general public is entirely skeptical of the security of their own data. There are privacy and civil liberties concerns sort of at every turn, whether you're talking about large ISP providers, commercial providers, or the government. How do you address those concerns? Because without addressing them, you can't get public support and buy-in. How do you address the privacy and civil liberties concerns as you look at this critical infrastructure, federal networks going forward?

MR. BOSSERT: Yeah, it's really a matter of trust, isn't it? I would be – I would be remiss if I didn't reiterate the importance of privacy and our respect for it and respect for those people who demand it. It is very difficult to say that knowing those people are very distrustful of large institutions. I joke sometimes I don't like lawyers, I don't trust the federal government, and here I am a lawyer working in the federal government. So I don't – I'm self-loathing, in some way.

That said, I think that healthy distrust of large institutions – and the federal government being the largest – is understandable, but I'm going to have to work very hard by being trustworthy, by being honest and candid and earning that trust back – and the president will and others will – in order to gain any kind of privacy concession. And there's no such thing as a concession in this game, but there's a

concession of trust, that we won't violate what people expect to be their core privacy expectations. And really, this is a matter of trust, and I'm going to do everything I can to earn that trust.

Now, that said, there's policies that we can put in place that would make that easier. There are policies we can put in place that will be less aggressive in some places. But I will not – I will not sit here and promise you that we'll be less aggressive in terms of law enforcement. There's going to be a lot of debates over things like encryption, over difficult topics that have no real answer, and there will be people that don't trust me or don't trust the administration. I think that's something that they should keep to themselves and hold and reserve judgement until they have some reason not to. I have not violated anyone's trust, and neither has the president. He has kept his word, and we've implemented a number of promises. He'll continue to govern responsibly, and I will continue to help him coordinate the interagency process responsibly. But as we struggle through those issues, trust is the issue.

In addition, law enforcement has a real responsibility. So now that I've said all that, let me be candid and tell you where I come from on this. We have to give law enforcement the tools they need to take bad people, whether they're terrorists or cyberhackers meant – or nation-states seeking to do us harm, and we need to stop treating them in a way that mollycoddles them. We have a responsibility to stop focusing on the victim of this stuff. It's not a Home Depot issue. It's not a Target issue. It's not an OPM issue. It's the issue of the person who has intentionally sought to do us harm, and we need to start turning around the messaging on that matter, and I have no problem saying that. The tools we use are directed at them, not directed at the innocent citizens of this country.

MS. TOWNSEND: Well, that's a perfect segue into so how do you engage – what is your view of how you engage nation-state actors? Multilaterally? Bilaterally? Some are sort of our greatest cyber advisories, whether it's China or Russia. The Chinese have offered the notion of a multilateral agreement that many view as binding U.S. options. How do you begin to tackle this sort of at the nation-state level?

MR. BOSSERT: Yeah. Yeah, carefully.

MS. TOWNSEND: (Laughs.)

MR. BOSSERT: Carefully. I've got great confidence, as does the president, in Secretary Tillerson, and you should know that cybersecurity is something that's very much on his mind. We will have engagements with friends, enemies, adversaries.

I think norms – you need to hear the word "norms" come from my lips. Norms are important. They are our statement, as a country – as the country that invented the internet, by the way – they are our statement that we have a certain expectation for how people will behave themselves on an open, interoperable platform that allows for innovation, free trade, fair trade, and other things that we think are important to our societal organization, socioeconomic organization. So those norms are important, and I think that's what you start with. You start by candidly telling other countries how we expect them to behave and how we promise to behave in return. And if they can – if they accept those norms and then fail to abide by them, we have a responsibility to call them out on it and we have a responsibility to do something about it. Now, I don't want to rush to putting anyone on notice or doing anything worse. What we have to do is start by establishing those norms, establishing evidence that they've violated those norms if they so choose, and then taking the appropriate steps to penalize and disincent that behavior. I think that's how you do it.

And I think that those countries – maybe another statement that might gain some attention here – I think those countries that are seeking data localization are misguided, and I think that that would be the ultimate logical outgrowth of any country – we won't do this for this reason in the United States – that seeks to increasingly centralize the role of cybersecurity for everyone. If it's a centralized function on behalf of the people run by the government, you'll have tendencies surrounding data localization and the exclusion from our markets of other services and goods from other countries. Those are two things that are antithesis to our – to our fundamental U.S. values, if you will. So I think those are the things. Those are the norms. Those are the expectations. Those are the how you call people out, as you would with any other human interaction. And then, lastly, I think kind of reiterating our value set in terms of a socioeconomic trade-based doctrine or a fair trade-based doctrine is the right way to go.

MS. TOWNSEND: So you mentioned penalizing those who don't observe kind of accepted norms of practice in cybersecurity. Is the administration willing to consider or look at the possibility of sanctions and that sort of regime to penalize those actors who don't observe those norms?

MR. BOSSERT: You know, I'm going to sound a little trite when I say this, but President Trump is absolutely focused on national security from an "America first" perspective and not in a way that is meant to harken back to some poor decisions or some historic anomaly. He is looking at this from the most honest perspective you can look at it. So if sanctions are appropriate and effective, I would have no problem recommending them to him. None, yeah. But that's getting way in front of ourselves right now. I think there's also some very positive opportunities for us to continue constructive conversations from Asia to the Middle East to our allies in Western Europe. And I think those are very positive conversations, for what it's worth.

MS. TOWNSEND: Yeah.

MR. BOSSERT: Yeah.

MS. TOWNSEND: So the private sector, many of whom are in this room, offer a bridge. And President Trump has been quite open to real – to engaging the private sector in – on public policy issues. Prior administration, President Obama, had a Silicon Valley initiative. How do you – what is your view and what's the president's view going forward about engagement with Silicon Valley on the very challenges you're facing?

MR. BOSSERT: Yeah. I think there's two answers to that, right? I don't want to be accused of being an institutionalist, but the first answer for me is to take all the initiatives underway that I'll say I, quote, unquote, "inherited," but that were underway through transition, and to run them through a thoughtful process so that we can analyze that which was working versus that which was not working, as opposed to that which was orchestrated by President Obama and that which was orchestrated by President Bush or that which was orchestrated by President Trump. That's not the model. That's not the approach. President Trump has not expressed those sentiments.

What he said is, figure out what's working and keep doing it. And figure out what's not working and quickly and without reservation stop it. And you've got my political top cover to do so. And so that's a very liberating way to operate. But I don't want to do it in a piecemeal fashion where it's Tom Bossert making those decisions. And that's also not what he wanted me to do. What he'd like to do is do is to have us do it through a thoughtful, collaborative, analytic fashion. And that's what's going to happen.

So there are some efforts underway that I suspect will have some merit and be borne out on the other end of that assessment. And I suspect there'll be some that maybe don't receive the same priority treatment. But it's not my job to render that decision, at least without perfect knowledge. I try not to render any premature conclusions. After we have a thoughtful process in place, you'll see something that's a little bit more defensible as we move forward.

But on the general issue, or general matter of coordinating with Silicon Valley, which is really just a way of saying that coordinating with smart people that are innovators in private industry and motivated by profit and penalized by market, you know, losses – those are great people. So we have no problem coordinating with them, whatever their political stripe. They have bright ideas and they're welcome. They're encouraged, because they're going to inherit the cyber-earth. (Laughter.)

MS. TOWNSEND: (Laughs.) So, you know, I heard you speak earlier today at breakfast, but share with us your thoughts about – frankly – because I don't think people hear enough from the government in acknowledgement to the private sector about the real damage and lost opportunity from DDoS attacks.

MR. BOSSERT: Yeah, so I briefly alluded to that. I think there's a number of ways to slice this. My instinct, the president's instinct, is not to mandate or regulate this into some kind of grinding, costly output. The idea here on botnets is one issue that we confront, just one. That one keyboard actuator at one machine can launch one launch code that then turns thousands or hundreds of thousands of devices against one target – a bank – strikes me as something that we should not address at the bank level. Does that make sense? So if it's a mountain, we're at the base of the mountain. And I'd like to address it higher in the topography. Obviously, the top of the mountain is that guy at that keyboard. If we can find that guy and eliminate his privileges from the Internet, that would be great.

But in the interim, I think that those other component – I alluded to it – I mean, it can involve Facebook and Google and ISPs and all the players that are involved in this – not to single them out – all of them can collectively together – at least it's my technical understanding – in a voluntary way figure a method for identifying those botnet attacks by looking at that network traffic and shunting it a little bit more effectively. I think right now our approach is to have the ISPs shunt that traffic. And there's a cost to that, right? It's happening a little bit too close to the bank. It's having a cost in terms of capacity. It's also having an opportunity cost. And I think that there's a way for us to greatly reduce – I can't say eliminate – but greatly reduce the number of botnets in this country through voluntary coordinated effort. And this president's going to call for just that.

MS. TOWNSEND: Tom, can you explain to us a little bit what you – what your view is of the relationship between government actors like NSA and DHS in terms of helping critical infrastructure providers protect themselves, identify threats before they manifest themselves? How do you strengthen that relationship so it's more real-time and it's more effective?

MR. BOSSERT: Yeah, that goes back to how we're going to address cybersecurity in general, doesn't it? So I think the first step for me – and not to sidestep your question – but first step is, and the president's first step is, for us to ask the departments and agencies to figure out means and methods – under their existing authorities or whether they need new authorities or capabilities – to help the most critical of those critical infrastructure Section 9 entities, if you will, and to work with them. And not say how secure are you, but for us to work with them and say, how can we help you be more secure?

Now, if I were that guy sitting at your seat, what would I be writing right now? In that category of things I'd be writing down, well, that's a platitude, right? I understand it's a little bit of a platitude, but it's also an acknowledgement of the difficulty of the problem. And it's a little bit of a punt on the answer to your question, but it's also a recognition of the fact that we're not helping people in their cybersecurity problems by going to the bank, in my previous analogy. There's also going to have to be systems that are attached to their systems. We talk about HVAC providers that were the threat vector into large companies, right? There needs to be a thoughtful assessment of how those companies are attacked, what those threat vectors are, how cybersecurity works.

And we're going to end up in a logical outcome here, where I don't want us to make the mistake of being the federal government protecting everyone's cyber interests. I want us to be the federal government that helps everyone think through the cybersecurity challenge in a little bit more of a thoughtful way, higher on the topography. If we can come up with those solutions, and to encourage private solutions, and the authorize them. So often the government's in the way.

So it's a little punt on this issue. But it's also not a punt if you see the direction that the president will issue, part of the first step is to engage with those companies to figure out how we can help them. But there's five or six other steps into the category of critical infrastructure that are going to be unpleasing or displeasing to you for right now. At least, I won't give us what you want. But give us another 100 days or so – we're 60 days into it – and we'll have more detail to answer that question.

MS. TOWNSEND: So let me – let me ask you. You know, one of the big questions that's been much in the press and has been a dogged concern, again, across administrations, is how do you get your arms around and tackle the insider threat? And frankly, even if the government could solve this for the federal government, it relies on the private sector and it relies on contractors. And so this has been another, you know, decades-long persistent threat. We haven't mentioned it yet this morning, but it must be part of your thinking and something that you have to address.

MR. BOSSERT: It's been quite a bit of my thinking recently. OK, two answers, not to be glib. The first answer, on insider threat, is that we have a responsibility – anybody who has an insider has a responsibility, and the federal government's one of them, to institute controls that are appropriate, to institute hiring practices that are appropriate, to reexamine them regularly. These are things that are common in their sense, but they need to be repeated regularly. And people inheriting new institutions often don't think of those rules, procedures and hiring practices. It's important.

But secondly – and this is something I care a little bit – a little bit about here with some passion. We need to find the people that do it and hold them accountable, and be absolutely unwavering in doing so. The people that have taken in the past things that they should not have taken, right, Snowden and others, are absolute enemies to our state – period. They need to be – they need to be caught, punished, and treated as such. I get head nods. Does anyone disagree with that? (Laughter.) Let me poll the audience. If people feel like they can continue to get away with it, they will. They cannot continue to get away with it.

You know, we have this responsibility in our security backgrounds, Fran and I, we've signed our names on so many things now I'm not sure what I can talk about anymore. And you've all been in that position as well. We have an affirmative responsibility in how we treat classified information to not only treat it appropriately, but if we're aware of someone else not treating it appropriately we have an affirmative responsibility to turn that person in.

I would remind everyone in this room that if you're a good patriot that you apply that same standard whether you've signed that piece of paper or not. If you see something, say something. It's a little trite, but it applies to cybersecurity as well. And we've all seen people and we've all known people that are not applying the right standard. But we've all also suspected there might be people that, you know, aren't exactly protecting our crown jewels the way they should. I have no tolerance for it. Neither does President Trump.

MS. TOWNSEND: So let me – I'll take it one step further. Let me suggest it's not only to individuals, but to those businesses that are doing – have the privilege of doing work and contracting for the federal government, they too might be held accountable and they too might suffer consequences if they haven't done the vetting of their own employees who turn out to be the insiders who threated federal information and leaked it, because while we're holding – while we talk about holding individuals accountable, the big Beltway contractors don't want to think that they could be threatened in terms of their commercial. And that's just another potential tool in the federal toolkit.

MR. BOSSERT: I think that's right. I think that's right. When we say "they" though, right, those organizations that have a responsibility – to the first part of my answer – they have a responsibility to hire properly, to institute practices and procedures that guarantee in some ways that they're not negligent in their hiring practices and their personnel practices. But then there's the person who might break those rules anyway. That person I have no tolerance for. The organization, both the government and our contractors, we have to do what we can do to maintain appropriate trust of our shopkeepers, so to speak.

MS. TOWNSEND: Thank you, Tom. Please help me in thanking Tom. We're going to let him get back to work. (Applause.)

MR. BOSSERT: Thanks.

JAMES A. LEWIS (Senior Vice President, CSIS): Thank you. Well, Tom told us earlier that in the 60 days he's been called a warmonger, an institutionalist and a technocrat – which is pretty good – a pretty good start –

MR. BOSSERT: I deny all three. (Laughter.)

MR. LEWIS: Yeah. But I think – I hope you all agree that he was really a good speaker and we got a lot of meat out of today's thing.

Fran, you've been an inspiration and a leader to us for a long time. Thank you for doing this.

MS. TOWNSEND: Thank you.

MR. BOSSERT: Could I thank you very much and make one more prerogative statement here? A small thing. Please don't focus on the executive order. Please focus on our conduct and behavior. That's more important. And the president's priorities speak for themselves. He's made cybersecurity a priority in his first 60 days several times, privately and publicly.

And then please also, in terms of the rumor mill that we all engage in, please note that I'd like you to welcome Rob Joyce as he joins the White House National Security Council team. For those of you that speculate he'll be joining, I'm honored to confirm that rumor. And we'll welcome Rob as

soon as the process can work its way through. But he will be an absolute treasure for me and for us and for the president as he coordinates these efforts.

So, Jim, thank you so much.

MR. LEWIS: Thanks, again.

MR. BOSSERT: Appreciate it. (Applause.)

MR. LEWIS: Thanks Fran. Go ahead.

(END)